REMARKS

Applicant respectfully traverses and requests reconsideration.

As a preliminary matter, Applicant notes that claim 35 was mis-numbered and as such the claims have been amended for proper renumbering.

Claims 1-6, 9-14, 17-25, 28-34 and 37 stand rejected under 35 U.S.C. §102(b) as being anticipated by Chan et al. (U.S. 2002/0019941A1). Chan describes a method and system for secure running of untrusted content. In Chan, restricted execution contexts are provided for untrusted content such as email messages and any attachments thereto or other information, for example, client processes that are run on a server. A restricted process is set up for the untrusted content and actions attempted by the content are subject to the restrictions of the process, which may be based on various criteria. Whenever a process attempts to access a resource, a token associated with that process is compared against security information of that resource to determine if the type of access is allowed. The security information of each resource determines the extent to which the restricted process, and thus the unrestricted content, has access. The criteria used for setting up restrictions for each untrusted content process is information indicative of how trusted or untrusted the content is likely to be. Chan is directed to a system that can protect against unruly executable content that is downloaded, for example, from the Internet. (See for example page 1, para. 0005.) The Chan reference does not appear to teach or suggest the claimed method or apparatus since among other things, it does not appear to determine a digital signature verification error such as verifying a digital signature of a certificate based on a received message header identifier associated with a public key certificate identifier.

For example, the office action cites page 8, second column, third paragraph and page 9, first column, first paragraph and page 10, first column, second paragraph of the Chan reference for this proposition. However this portion, for example, does not appear to be directed to a

digital signature verification process or the detection of an error based on a digital signature verification process based on a received message header identifier associated with a public key certificate identifier. Instead, the cited portion refers to a calling process being checked to see if it is restricted by an appropriate restricted security identifier in a token. However, as understood, it does not appear to be performed by a digital signing verification process that is based on a received message header ID that is associated with a public key certificate identifier as required by the claim. In fact, it does not appear that the described token is digitally signed nor does it appear that a message header identifier that is associated with a public key certificate identifier is used in any digital signature verification process. As such, the claims are in condition for allowance. If the rejection is maintained, Applicant respectfully requests a showing as to which data in the cited reference corresponds to, for example, the received message header identifier associated with the public key certificate identifier, the digital signature of what entity is being verified and which entity perform such digital signature verification and based as an error detection performs the step of generating a digital signature verification map.

In addition, the reference also appears to fail to teach generating a digital signature verification map that contains a plurality of acceptable message header identifiers associated with the public key certificate identifier. The office action cites to page 8, first column, third paragraph and page 9, second column, third and fourth paragraphs. However, as best understood, paragraph 0082 of the cited reference describes for example, that a URL string is converted to a restricted security ID through a one-way cryptographic hash function to convert the URL string to a restricted security identifier by adding a header indicating that the number is a security ID identifier and how the number was generated. In the instance where a binary certificate identifier is available for a particular website, then the binary certificate ID is used to

generate the restricted SID. As such, this portion describes generating a security ID. There is no digital signature verification map that includes a plurality of acceptable message header identifiers that is associated with the public key certificate identifier. In fact, it does not appear that any digital signature verification operation is described nor is there a reference to a plurality of acceptable message header identifiers that are contained in a digital signature map as required by the claim. Accordingly, the claims are also in condition for allowance based on this reason as well.

Moreover, the portion in page 9, such as paragraph 0093 and 0094 refer to a sender sending an email message and that the email may include a digital signature that may be used to verify that the sender is the source of the message. However, again there is no digital signature verification map that is generated nor any digital signature verification map that contains a plurality of acceptable message header identifiers that are also associated with public key certificate identifiers. As such, the claims are believed to be in condition for allowance.

As for claims 2, 5, 21, 24, 30 and 33, Applicant respectfully reasserts the relevant remarks made above and also respectfully submits that the cited portion of the reference appears to simply refer to the fact that a restricted security ID is placed in a restricted security ID field of a restricted token wherein the restricted security ID may be a hash value that may include a certificate identifier of a website. However, again there does not appear to be any generation of a digital signature verification map that stores an acceptable message header identifier as a map entry in response to determining the digital signature verification error. For example, there does not appear to be an updating of a digital signature verification map when a digital signature verification error is determined. To the contrary, since there is no digital signature verification

error being determined based on a received message header identifier, the claims are in condition for allowance.

As to claims 3, 22 and 31, Applicant respectfully reasserts the relevant remarks made above with respect to the relevant independent claims and also respectfully submits that the cited portion fails to describe mapping of a plurality of acceptable message header identifiers on a per certificate subject identification databases. Again, since there is no determination of a digital signature verification error and a subsequent generating of a digital signature verification map, these claims are also believed to be in condition for allowance.

As to claims 4, 10, 12, 18, 23 and 32, Applicant respectfully reasserts the relevant remarks made above with respect to the relevant independent claims and also again note that the cited reference does not appear to generate a digital signature verification map that contains a plurality of accepted message header identifiers associated with the public key certificate identifier after determining that a digital signature verification error has occurred. As such, there is no verification of a digital signature based on a digital signature verification map as required in these claims. Accordingly, these claims are in condition for allowance.

As to claims 6, 14, 25 and 34, Applicant respectfully reasserts the relevant remarks made above with respect to the relevant independent claims.

As to claims 9, 11, 13, 19, 28 and 37, the office action cites page 8, second column, third paragraph as teaching that a step of determining a digital signature verification error includes comparing the public key certificate identifier with a mismatch as detected. However, the cited portion of the reference does not teach comparing a public key certificate identifier with the message header identifier to determine if a mismatch is detected. In fact, the only reference to a certificate is the binary certificate ID. However, this portion teaches that such a binary

certificate ID is used in a hash function to generate the restricted security ID. There is no comparison of a public key certificate identifier and message header identifier to determine if a mismatch is detected. Moreover, the claim requires that if a mismatch is detected, then a mismatch notification is generated for an operator and a digital signature is verified based on a verification key associated with the public key certificate identifier. No such mismatch notification appears to be taught or suggested nor a verification process as claimed. As such, this claim is also believed to be in condition for allowance.

Claims 7, 15, 26 and 35 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Chan. It appears that the office action admits that Chan fails to disclose a digital signature of a digital signature verification map to provide a trusted digital signature verification map. However, another section of Chan has been cited as allegedly being properly combinable to render Applicant's invention obvious. The cited portion in Chan is directed to the digital signature of an email message to ensure that the message is trustworthy. However, it also appears that the office action is attempting to equate a digital signature verification map with the "restricted token" in the Chan reference. However, as noted above, there is no digital signature verification process that is used to generate the restricted token in a manner as claimed by Applicant. Accordingly, the claims are in condition for allowance based on the reasons given above. Moreover, using selected portions of the Chan reference thereof to render Applicant's claimed invention obvious does not appear to be proper since there is no motivation to combine disparate teachings. In fact, if it was obvious, it is curious why Chan did not describe such a system. For example, as admitted by the Patent Office, the restricted tokens as described in Chan do not appear to be signed by any trusted authority, yet Chan describes elsewhere that emails are digitally signed. Accordingly, Chan did not contemplate utilizing a digitally signed

restricted token and as such, using Applicant's invention as a roadmap appears to be improper. For these reasons also, the claims are believed to be in condition for allowance.

Claims 8, 16, 27, 36, 38 and 39 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Chan in further view of Cooper et al. (U.S. 006052442A). Applicant respectfully reasserts the relevant remarks made above with respect to the Chan reference and also notes that these claims require, for example, "generating a trusted alias map containing a plurality of acceptable message identifiers in at least one associated subject alias" as such, the alias map described must be trusted. In addition, the claim requires, for example, displaying a subject alias that it is in the trusted alias map in response to verifying a digital signature associated with the public key certificate identifier. The office action admits that Chan fails to among other things, disclose a generation of a trusted alias map and the display of at least one subject alias that is in the trusted alias map. Cooper has allegedly been cited as teaching these steps.

However, Cooper appears to be silent as to providing any trusted map, let alone a trusted alias map. Cooper does not appear to contemplate digitally signing or otherwise making an alias map trusted. For example, Cooper is directed to an Internet answering machine that when the answering machine detects a ring signal on a telephone line, it answers the call. The answering machine plays an outgoing message for the caller to hear and records that caller's incoming voice message. Periodically, the answering machine may check for email messages by calling a service provider. When the service provider answers the call, the answering machine logs in, downloads and stores email messages that have been received. A user can then view and display and review the messages. Cooper does not appear to be directed to a method for providing information security as required by the claims nor to a system that employs trusted alias maps as

required by the claims. For example, the cited portion of Cooper, namely page 9, first column, second and sixth paragraphs and column 10, first paragraph, describe, for example, that a caller's name may be converted using a telephone number such that a telephone number is translated to a pneumonic tag. In a similar manner, an email address that is received may be converted into a tag and may be displayed in place of or in addition to the email address. These tags are not stored or represented in a trusted manner nor is there any discussion or teaching of providing a trusted alias map containing acceptable message identifiers in at least one associated subject alias. Accordingly, the claims are believed to be in condition for allowance.

Accordingly, Applicant respectfully submits that the claims are in condition for allowance and that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: 4/2/04

By: _____
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P. C.
222 N. LaSalle Street
Chicago, IL 60601
PHONE: (312) 609-7599
FAX: (312) 609-5005
E-MAIL: creckamp@vedderprice.com